

Florida Local Government Cybersecurity Grant Frequently Asked Questions

Go to CyberGrants.FL.gov to access the Florida Local Government Cybersecurity Grant Application.

Florida Local Government Cybersecurity Grant

Q: What is the Florida Local Government Cybersecurity Grant?

A: The Florida Local Government Cybersecurity Grant is a competitive grant program to provide cybersecurity technical assistance to local Florida governments to improve their cybersecurity posture and resiliency.

Q: Is the FL[DS] (Florida Digital Service) providing assistance?

A: Yes. The State of Florida's FY 2022-2023 GAA includes an appropriation for cybersecurity technical assistance, which will be administered by the FL[DS].

Q: When can we apply?

A: The application period is from February 16, 2023, through March 31, 2023.

Q: How do I apply?

A: Go to CyberGrants.FL.gov and click the button for the Online Grant Application, near the bottom of the page. Your organization should complete **one** application and provide two points of contact at a minimum. One contact to serve as an Executive Sponsor and one contact as a Primary Contact for the grant application.

Q: Can I save my application and return later to submit?

A: Entities are required to complete their application once it has been started. A full version of the application is available on the [home page](#). You can use this PDF version to collect all the required information before starting the submission process.

Q: How do I find further guidance or information?

A: Go to CyberGrants.FL.gov where a timeline is available providing information on upcoming technical webinars and other events. Additionally, you can reach out for technical assistance through the Slack channel or via email at cybersecuritygrants@digital.fl.gov

Available Assistance

Q: What type of assistance is available?

A: Assistance will be provided in the form of capabilities. Examples include software licenses, tools, and support resources. Information on the capabilities provided is available on the [homepage](#) in the additional resources section.

**Florida Local Government Cybersecurity Grant
Frequently Asked Questions**

Q: What is the term of the grant?

A: If awarded, the grant will be for a period of 12 months, depending on the capabilities requested by the applicant.

Q: If awarded, will we continue to receive capabilities longer than the initial 12-month period?

A: If additional funding is received in the upcoming fiscal year, FLDS intends to extend and renew current agreements with awarded applicants.

Q: How do I receive funding assistance instead of capabilities?

A: The FL[DS]'s primary focus is enabling local entities with capabilities that integrate with the State's Cybersecurity Operations Center. This allows the FL[DS] to purchase at scale, provide an enterprise support model, provide Incident Response services, and monitor for threats and vulnerabilities. However, if there are critical needs that cannot be met by providing capabilities (existing or future), we would love to know about them in consideration of this grant opportunity. Feel free to document these needs in the Additional Needs section of the application; instructions are provided.

Q: What if I do not need any of the capabilities offered, but have other critical needs?

A: If there are cybersecurity capabilities specific to your organization you would like us to consider, please provide information through the grant application about the need and its criticality, the solution and its projected impact, the estimated cost, and how you would procure, manage, and integrate the solution with the State Cybersecurity Operations Center. Provide sufficient information to establish goals for award, to demonstrate performance post-award and explain how the capability avoids creating siloed architecture by integrating with the state CSOC. You may upload any supporting documentation in the attachments section labeled as Additional Needs.

Q: Will my organization have control over these capabilities?

A: The FL[DS] will deliver a solution for your operation and will adhere to the principle of least privilege and multi-tenant design. FL[DS] will only have access to the specific data, resources, and applications needed to enable your organization with the agreed upon capabilities you request and are awarded. You are encouraged to review the sample riders, agreements, and warranties that were purposefully crafted to protect your organization's privacy and sovereignty. They can be found on the [homepage](#) in the additional resources section.

Florida Local Government Cybersecurity Grant Frequently Asked Questions

Eligibility

Q: What is considered an “eligible entity?”

A: Proviso includes the following information regarding eligible entities:

Funds in Specific Appropriation 2944A from the General Revenue Fund are for local government cybersecurity technical assistance grants. The Department of Management Services shall administer the competitive grant program, and the State Chief Information Security Officer shall develop the criteria and process for awarding such assistance funds to municipalities and counties.

Q: Are there any additional requirements for eligibility?

A: An entity that is approved for award must complete the below signed agreements with FL[DS] within 30 days of award:

- Data Sharing Agreement
- The Incident Response Rider
- The Software Specific Rider(s)
- Grant Agreement

Examples of these agreements can be found on the [homepage](#) in the additional resources section.

Verification and Documentation

Q: How is an entity verified?

A: Upon submission, we will review your application to determine if your organization is eligible for this grant opportunity. Even if you are unsure of your organization’s eligibility, we encourage you to submit an application. This will help inform us of the needs for future grant opportunities and to whom they should be aligned.

Q: What does it mean to manage critical infrastructure?

A: Critical infrastructure is defined by 60GG-2.001(2)(a)10., Florida Administrative Code - systems and assets, whether physical or virtual so vital to the U.S. that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. Per the Department of Homeland Security, critical infrastructure can include communications, chemical, commercial facilities, critical manufacturing, dams, defense industrial base, emergency services, energy, financial, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactors/materials and waste, transportation systems, and water.

Application Process

Q: When will I get the requested assistance?

A: Awards will be announced mid-April 2023. Rollout of capabilities will follow within a month of award.

**Florida Local Government Cybersecurity Grant
Frequently Asked Questions**

Q: How will I know if I do not qualify for this assistance?

A: Applicants who do not qualify for assistance or who did not receive an award will be notified via email.

Q: Why was my application not approved?

A: The application can be denied for three reasons:

1. The application is incomplete and further information was not provided when requested.
2. The entity type does not categorize as an eligible entity.
3. The application provided invalid information.
4. Funding was fully expended on other entities that were a higher priority for this grant.